

- a. a name identifier of a signer
- b. a statement of the current date and time at the time of signature
- c. a generated nonce
- d. a network address for the signer
- e. a credit card authorization
- f. one or a plurality of properties of a digital certificate of the signer
- g. an email address of the signer
- h. a representation of one or a plurality of biometric identifiers of the signer
- i. a unique identifier of a signature transaction.

81. The method of claim 79 whereby data to be signed is furnished to a remote computer for signature.

82. The method of claim 81 whereby the data consists of textual or binary data that is transmitted via one, or a plurality of inputs, of one, or a plurality of forms, to the remote computer.

83. A method for a remote computer to electronically sign data comprising:

- a. where authentication of a signer's identity is established or is not required, a means of transmitting data, or a message digest thereof, to the remote computer for signature;
- b. a means to encrypt a message digest of the data using a key not belonging to the signer; and
- c. a means to associate the signer with the signature.

84. The method of claim 83 wherein an encrypted message digest is a detached digital signature.

85. The method of claim 85 wherein the detached digital signature is encrypted by means of a symmetric key.
86. The method of claim 83, wherein data that associates the identity of an authorized signer with the entity's digital signature is a signature transaction record consisting of a message digest and encrypted message digest of the data, and optionally, one or a plurality of the following;
- i. a date of signature,
 - ii. a time of signature,
 - iii. a generated nonce,
 - iv. a credit card authorization,
 - v. a network address from whence a request to sign originated,
 - vi. the signer's name identifier;
 - vii. a unique identifier assigned to the signature transaction record;
 - viii. an email address of the signer;
 - ix. one or a plurality of properties of a digital certificate issued to the signer;
 - x. a representation of one or a plurality of biometric identifiers of the signer.
87. The method of claim 86 wherein the symmetric key is derived from a password or seed of composed of one or a plurality of values, or message digest thereof, contained in the signature transaction record.
88. The method of claim 83 whereby a digitally signed confirmation of a signature transaction is transmitted to a signer from a remote signing computer as proof of an authentic signature transaction.
89. The method of claim 88 whereby upon receipt, the proof of an authentic signature transaction is subsequently signed by a recipient using a private asymmetric key associated with a digital certificate of the recipient as an act of signature.

90. The method of claim 83 wherein the message digest is encrypted by means of a symmetric key.
91. The method of claim 91 wherein the symmetric key is derived from a password or seed of one or a plurality of values, or message digest thereof, contained in the signature transaction record.
92. The method of claim 83 wherein the data submitted for signature consists of one or a plurality of the following:
- a. data that is supplied by a user to a remote computer through submission of one or a plurality of inputs to one or a plurality of forms,
 - b. data that is supplied by a user to a remote computer through submission of one or a plurality of inputs to one or a plurality of forms, in combination with a template supplied by a remote computer,
 - c. a file,
 - d. a message,
 - e. a document,
 - f. a message digest,
 - g. transaction data,
 - h. XML data,
 - i. programming code,
 - j. a document containing mark-up,
 - k. one or a plurality of units of currency,
 - l. a legal document,
 - m. a medical record,
 - n. a prescription,
 - o. a promise,
 - p. a promissory note,
 - q. a contract,
 - r. a mortgage or deed of trust,

5
don't

- 11
cont
- s. a purchase order,
 - t. text,
 - u. one or a plurality of numbers,
 - v. a conveyance,
 - w. a transaction record,
 - x. one or a plurality of dates,
 - y. a check or money order,
 - z. binary data.

93. The method of claim 83 whereby upon a successful signature verification, the remote computer sends a digitally signed message as proof of a verified signature transaction.

94. A method for signing by or on behalf of an entity by one or a plurality of authorized signers consisting of the following:

- a. where authentication of a signer's identity is established, a means of digitally signing data by a remote computer using a key of the entity; and
- b. a means to associate the identity of a signer with the digital signature of the entity.

95. The method of claim 94 wherein an association between the identity of an authorized signer and the entity's digital signature is established by the symmetric encryption of the entity's digital signature with a key generated from a password or seed derived from one or a plurality of the following, or message digest thereof:

- a. a name identifier of the authorized signer;
- b. an email address of the signer;
- c. a representation of one or a plurality of biometric identifiers of the authorized signer.

96. The method of claim 94, wherein data that associates the identity of an authorized signer with the entity's digital signature is stored as a signature transaction record in a database for use in verifying a signature.
97. The method of claim 94, wherein data that associates the identity of an authorized signer with the entity's digital signature is stored as meta-data in a document for use in verifying a signature.
98. The method of claim 94 wherein a message digest of the data to be signed is transmitted to a remote computer, which asymmetrically encrypts the message digest using a private key of the entity to generate the entity's digital signature.

Very respectfully,


John H. Messing
Applicant Pro Se

3900 E. Broadway Blvd., Suite 201, Tucson, AZ 85711 (new address)

Tel.: (520) 547-7933

Fax: (520) 547-7920

Certificate of mailing: I certify that on the date below this document and referenced Second Substitute Specification and referenced Second Substitute Specification Mark-up and attachments were deposited with the U.S. Postal Service as first class mail in an envelope addressed to: "MAIL STOP NON-FEE AMENDMENT, ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231."

June 5, 2003


John H. Messing
Applicant